Configuration Manual

Ascom i75 VoWiFi Handset

2008-11-20/ Ver. B

Contents

1 Introduction

The Ascom Voice over Wireless Fidelity (VoWiFi) system provides wireless IP-telephony, messaging and alarm functions to enterprise LANs. Using third-party WLAN products as well as in-house developed hardware and software, the system enables data and voice transmission together with seamless roaming.

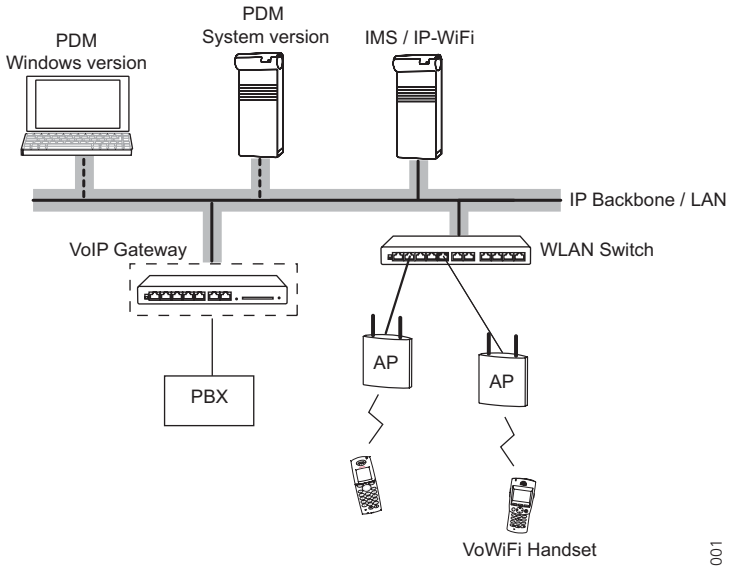

Figure 1. Ascom VoWiFi System

This document is intended as a guide when installing the Ascom i75 Handset in a VoWiFi system. The document describes the settings needed to make the i75 Handset function in a VoWiFi system and is relevant to the following personnel:

- System Administrator
- Service Technician

It is assumed that the reader of this document has basic knowledge of the Ascom VoWiFi system.

1.1 Abbreviations and Glossary

AP	Access Points
DHCP	Dynamic Host Configuration Protocol
DTIM	Delivery Traffic Indication Message
ELISE	Embedded LInux SErver: A hardware platform used for Unite modules
ESS	Enhanced System Service: Unite module that handles centralized number planning, remote connection, system supervision, fault handling, group handling, message routing, centralized logging, activity logging, and user access administration.
ESSID	Extended Service Set Identifier
ETSI	European Telecommunications Standards Institute
IMS/IP-WiFi	Integrated Message Server
MWI	Message Waiting Indication
NTP	Network Time Protocol
PDM	Portable Device Manager
PRI	Primary Rate Interfaces
PTT	Push-To-Talk
QoS	Quality of Service: Defines to what extent transmission rates, error rates etc. are guaranteed in advance.
VoWiFi	Voice over Wireless Fidelity: Is a wireless version of VoIP and refers to IEEE 802.11a, 802.11b or 802.11g network.
WLAN	Wireless Local Area Network

2 Pre-Installation

Before installing Ascom i75 handsets in a VoWiFi system, make sure that all equipment is available. It is recommended to set up battery chargers and charge the handset batteries before installation, and to have a number plan available for the handsets.

We assume that the VoWiFi system is installed including some or all of the following components (depending on system configuration):

- VoIP Gateway. This is the gateway for ISDN primary rate interfaces (PRI) in the Ascom VoWiFi and IP-DECT systems. It serves as a link between traditional telephony and VoWiFi telephony.
- Portable Device Manager (PDM). The PDM is used for administration and programming of the i75 VoWiFi Handsets and exists in two versions, the *PDM Windows version* and the *PDM System version*.

  For effective administration of a VoWiFi system with several handsets, it is required to have both PDM versions. The PDM Windows version is only used to allow the handset to access the WLAN system. All other settings and updates are done with the PDM System version.

  In small systems it is possible to administer the system only using the PDM Windows version. All settings and updates are in this case done from the PDM Windows version via the USB programming device.
- IMS/IP-WiFi. The IMS/IP-WiFi is required when using PDM System version. The IMS/IP-WiFi handles all communication between the WLAN and the PDM System version. Before installing the handset make sure the IMS/IP-WiFi IP address is available.
- DHCP Server. A DHCP server allows devices to request and obtain an IP address from a server which has a list of addresses available for assignment. If the WLAN system does not have a DHCP server, a list of static IP addresses is necessary.

2.1 VoWiFi System IP addresses

Complete the table below with the IP addresses, as a help when configuring the handsets.

Device	**IP address**	**Required**
VoIP Gateway		Yes
PDM System version		Yes
IMS/IP-WiFi		Yes
Subnet Mask		Yes
Number plan	N/A	Yes
NTP Server address[a]		
DNS Server address[a]		
Central Phonebook		If used
ESS		If used
DHCP range		

a. Depending on system configuration

3 Programming the Ascom i75 VoWiFi Handset

The programming of the i75 VoWiFi Handset is done by using the Portable Device Manager (PDM) which exists in two versions, the *Windows* version and the *System* version.

3.1 PDM Windows version

The Windows version is run on a PC. Program the handset via the PDM Windows version by connecting the USB Programming Device to the computer with the USB cable, start the PDM, and then place the handset in the USB Programming Device.

For instructions on how to use the PDM Windows version, see *Installation and Operation Manual, Portable Device Manager (PDM), Windows version*, *TD 92325GB*.

3.2 PDM System version

The System version is run on an Elise module and via a java client PC connected to the LAN. In this case the handset is programmed over the air.

For instructions on how to use the PDM System version, see *Installation and Operation Manual, Portable Device Manager (PDM), System version*, *TD 92378GB*.

4 Handset Installation

This section describes the recommended procedure to install several handsets in a large system and to install a few handsets in a small system. There are several ways to install a handset but the procedures described here guarantees simple maintenance of the system.

The procedure differs depending on the size of the system. For effective administration it is recommended to use the PDM System version, but in small systems it is possible to administer the handsets using only the PDM Windows version.

Installation steps in large VoWiFi Systems:

1 Create templates in the PDM System version; one with network settings and another with common settings.

2 Create user numbers (handsets) and apply the templates.

3 Create a template with identical network settings in the PDM Windows version (for log on of the handsets).

Installation steps in small VoWiFi Systems:

1 Create user numbers.

2 Create one template for all settings in the PDM Windows version.

4.1 Installation in Large Systems

When installing several handsets in a VoWiFi system, it is required to have both the PDM System version and the PDM Windows version to make the maintenance and handling of the system as simple as possible.

4.1.1 Create a Network Template in the PDM System version

Create one template which contains the network settings only. This must be done to prevent the PDM System version from restoring the WLAN parameters to default during the first synchronization.

Note: Only select the parameters that are changed, if all parameters are selected the system performance decreases

1 Open the PDM System version.

2 Create a template with the network parameters:

- ESSID
- WLAN settings[1]
- IMS IP address

3 Save the network template in the PDM System version using a descriptive name.

4.1.2 Create a Common Template in the PDM System version

Create another template with the common settings (exclude the network settings) applicable to all handsets. This template contains for example, hidden menu items in the display, certain level of ring signal and vibrators.

1. All required system settings for the WLAN. For example Security mode and Encryption type.

Note: Only select the parameters that are changed, if all parameters are selected the system performance decreases.

1 Open the PDM System version.

2 Create a template with the specific parameters. See section *8 Configure the Ascom i75 VoWiFi Handset* on page 13 for more information.

3 Save the template in the PDM System version using a descriptive name.

4.1.3 Create User Numbers in the PDM System version

Create a range of user numbers (phone numbers) and apply the templates previously created in the PDM System version.

IMPORTANT: Do not add handsets that already exist in the system. The PDM System version will overwrite the existing parameters in the handset.

1 Open the PDM System version.

2 Add a range of user numbers.

3 Apply the *network settings* template to the selected handsets.

4 Apply the *common settings* template to the selected handsets.

5 Close the PDM System version.

Note: The parameter version of the template must be equal to or less than the selected parameter version.

4.1.4 Create a Network Template with Initial Configuration in the PDM Windows version

The handsets are activated using the PDM Windows version. Create a template with the basic network settings. This template is only used the first time the handset logs on to the VoWiFi System. After log in the settings in the handset are changed according to the templates in the PDM System version.

Note: The parameters in this template should be identical to the parameters in the network template created in the PDM System version.

1 Open the PDM Windows version.

2 Create a template with the following network parameters:

- ESSID
- WLAN settings[1]
- IMS IP address

3 Save the template in the PDM Windows version.

4 Put the handset in the USB programming device.

5 Run the template.

6 Remove the handset when synchronisation is finished. The handset is restarted and "Remotely updated" is displayed.

7 Enter the user number and leave the password blank to log in to the system.

Repeat step 4 – 7 for all handsets.

1. All required system settings for the WLAN. For example Security mode and Encryption type.

4.2 Installation in Small Systems

In a small VoWiFi system it is not mandatory to have both a PDM System version and an IMS/IP-WiFi installed. The administration can be handled with the PDM Windows version only.

The synchronization is in this case not handled automatically by the system. Each handset must be placed in the USB programming device connected to the administrators computer.

Tip: Create a template containing both network settings and common settings.

1 Open the PDM Windows version.

2 Create a user number or a range of user numbers. (Not needed if the numbers are created in the PDM System version.)

3 Create a template which contains at least the following:

- ESSID
- WLAN settings[1]
- (IMS IP address)
- Protocol
- Gatekeeper/SIP proxy IP address

4 Save the template.

5 Apply the template on the stored user number(s).

6 Put the handset in the USB programming device.

7 Associate the handset with the user number.

8 Remove the handset when synchronisation is finished. The handset is restarted and "Remotely updated" is displayed.

9 Repeat step 4 – 7 for all handsets.

1. All required system settings for the WLAN. For example Security mode and Encryption type.

5 System Maintenance

In an existing VoWiFi System it is important to be able to replace handsets, add new handsets and exchange faulty handsets. The recommended procedure is to use a temporary template with basic network settings for log in, created in the PDM Windows version, and then apply the templates created in the PDM System version.

Tip: Perform step 2-4 in chapter 5.1 or chapter 5.2 for a couple of spare handsets. Switch off the handsets when User name and Password are displayed. When, for example, a handset needs to be replaced, just switch on a handset and enter the number. The individual settings are automatically downloaded to the new handset.

Another important matter is to be able to upgrade system parameters and security settings in the handsets. These upgrades are preferably done in the PDM System version.

5.1 Replace Handset in a VoWiFi System

1 Open the PDM Windows version.

2 Put the handset in the USB programming device.

3 Run the template with the basic network settings containing:

- ESSID
- WLAN settings[1]
- IMS IP address

4 Remove the handset from the USB programming device.

5 Enter the user name and leave the password blank.

6 Press "Log on".

The handset is automatically updated from the PDM System version and restarted.

5.2 Add Handset to a VoWiFi System

1 Open the PDM Windows version.

2 Create a user number or a range of user numbers.

3 Put the handset in the USB programming device.

4 Run the "basic template" containing:

- ESSID
- WLAN settings[1]
- IMS IP address

5 Remove the handset from the USB programming device.

6 Apply the *network settings* template to the selected handsets.

7 Apply the *common settings* template to the selected handsets.

8 Enter the user name and leave the password blank.

9 Press "Log on".

The handset is automatically updated from the PDM System version and restarted.

1. All required system settings for the WLAN. For example Security mode and Encryption type.

5.3 Update the System Parameters

This section describes the general procedure on how to change/update parameters. The update starts when the handset is idle and will not interrupt an ongoing call.

Note: Only select the parameters that are changed, if all parameters are selected, the system performance decreases.

1 Open the PDM System version.

2 Create a new template with **only** the parameters that shall be changed.

3 Select the handsets that should be updated and apply the template.

The handsets are automatically updated from the PDM System version and restarted.

5.4 Perform a Security Upgrade

This section describes how to perform an update/change of the WLAN password/ authentication.

Tip: Leave one access point with the old configuration to allow switched off handsets to receive the updates.

1 Open the PDM System version.

2 Create a new template with the new security settings.

- Security mode[1]
- Encryption type[1]

3 Apply the new template to the handsets.

The handsets are automatically updated from the PDM System version and restarted.

Note: At this time, the handsets have no access to the WLAN system.

4 Change the security settings for the access points.

The handsets are now able to access the WLAN.

5.5 Using Shared Phone in the VoWiFi System

A handset that is shared changes its identity and settings depending on the User name entered when the handset logs in. All personal settings and the local phone book will be downloaded from the PDM System version.

Requirements:

- IMS/IP-WiFi
- PDM System version
- ESS (Optional)

The handset must be configured to be a shared phone, see section 8.5.4 *Phone Mode* on page 18 for more information.

A handset with personal mode may also use a shared password (empty or specific) from the IMS/IP-WiFi. For personal password, a User Server (ESS) is required.

1. All required settings for the WLAN. For example User name, Password, Regulatory domain etc.

Note: If you enter a personal phone number in the shared handset, the handset becomes personal because the record in the PDM System version will synchronize and change the settings in the handset.

5.6 Upgrade the Template

The upgrade procedure of the templates definition version is described in the applicable *PDM Installation and Operation Manual*.

5.7 Create a Configuration Backup

It is recommended to have a backup of the configuration in the handsets and the site.

The backup procedure is described in the applicable *PDM Installation and Operational Manual*.

6 Add Alarm Features

As default the basic alarm types; Emergency call after alarm, Test alarm and Push button alarm, are available for the user. For optional alarm features; No-movement and Man-down alarm, the i75 VoWiFi Handset requires a licence. The licence is activated from the i75 home page. The user name and password to the WLAN used for the i75 VoWiFi Handsets is required for the activation.

A licence can be downloaded from the Ascom Wireless Solutions Extranet and the IP address to the i75 home page can be found in the i75 handset menu. Ask the system administrator for the administration user name and password.

6.1 Upgrade

1 Download a licence number from the Ascom Wireless Solutions Extranet. Make a note of the licence number.

2 Enter the Ascom i75 handset menu, mark “Settings” and press “Select”.

3 Mark “System” and press “Select”.

4 Mark “Information” and press “Select”. Make a note of the IP address.

Tip: Enter the quick access code *#46# to view the system information directly without stepping in the menu.

5 Use a browser and enter the IP address. The *Ascom i75* internal web administration page opens.

6 Click on the “Alarm” link in the left pane. The *Enter Network Password* window opens.

7 Log in with the administration user name and password.

8 Enter the licence number in the “Licence number” text field.

9 Click “Activate”.

Additional functions have now been added to your handset. The functions can be used immediately without restarting the handset.

7 Add Location Features

To be able to transmit collected data to the 3'rd party location appliance, the i75 VoWiFi Handset requires a licence. The licence is activated from the i75 internal home page. The user name and password to the WLAN used for the i75 VoWiFi Handsets is required for the activation.

A license can be downloaded from the Ascom Wireless Solutions Extranet and the IP address to the i75 home page can be found in the i75 handset menu. Ask the system administrator for the administration user name and password.

7.1 Upgrade

1 Download a licence number from the Ascom Wireless Solutions Extranet. Make a note of the licence number.

2 Enter the Ascom i75 handset menu, mark "Settings" and press "Select".

3 Mark "System" and press "Select".

4 Mark "Information" and press "Select". Make a note of the IP address.

Tip: Enter the quick access code *#46# to view the system information directly without stepping in the menu.

5 Use a browser and enter the IP address. The *Ascom i75* internal web administration page opens.

6 Click on the "Location" link in the left pane. The *Enter Network Password* window opens.

7 Log in with the administration user name and password.

8 Enter the licence number in the "Licence number" text field.

9 Click "Activate".

Additional functions have now been added to your handset. The functions can be used immediately without having to restart the handset.

8 Configure the Ascom i75 VoWiFi Handset

The VoWiFi Handset requires some settings to function in the VoWiFi System. All settings are done in the PDM. This section describes the available settings for the handset.

For more information, see the PDM Online Help or the applicable *PDM Installation and Operation Manual*.

8.1 Select System

The handset can switch between 4 different system configurations. A handset belongs to 4 different WLANs but only to one IMS/IP-WiFi and VoIP Gateway. System A is default and used throughout this manual.

1 Select Device > User.

2 Select "A" in the *Active System* drop-down list.

8.2 IP Settings

The IP settings can be configured in two ways, either Automatic IP settings which means that the handset receives an IP address from a DHCP server, or Static IP settings which means that the IP addresses have to be entered manually.

8.2.1 Automatic IP Settings

1 Select System > A.

2 Select "Enable" in the *DHCP mode* drop-down list.

The Phone IP address, Subnet mask and Default Gateway are automatically set-up.

8.2.2 Static IP Settings

1 Select System > A.

2 Select "Disable" in the *DHCP mode* drop-down list.

3 Enter the IP address to the handset in the *Phone IP address* field.

4 Enter the subnet mask in the *Subnet mask* field.

5 Enter the IP address to the default Gateway in the *Default Gateway* field.

8.3 Network Settings

8.3.1 ESSID

The ESSID is the name of the network the handset associates to.

1 Select System > A.

2 Enter system ESSID in the *ESSID* field.

8.3.2 World Mode Regulatory Domain

There is a set of regional rules for the ISM 2.4GHz frequency band the handset complies to. The preferred setting is "World mode (802.11d)" where the handset listens before transmitting but it requires that the WLAN infrastructure supports this feature.

1 Select System > A.

2 In the *World mode regulatory domain* drop-down list, select one of the following:

- World mode (802.11d)
- Canada
- ETSI
- France
- Spain
- USA

8.3.3 Voice Power Save Mode

The voice power save mode is used during calls. ACTIVE is recommended to obtain optimal voice quality. U-APSD and PS_POLL uses less power but is more sensitive to network disturbances.

If supported by the infrastructure "U-APSD" is the preferred choice. U-APSD multiple the talk time more than 4 times compared to ACTIVE mode.

1 Select System > A.

2 Select one of following in the *Voice power save mode* drop-down list.

- ACTIVE
- PS_POLL
- U-APSD

8.3.4 802.11 b/g Channels

Defines which 802.11b/g channels to use. It is recommended to use the default value. If set to "All", all channels are scanned for access points which decreases the WLAN performance. Select "Advanced" only if the channels shall be set in the parameter *Advanced: 802.11 b/g channels*.

1 Select System > A.

2 Select one of the following in the *802.11b/g channels* drop-down list.

- All
- 1,6,11
- Advanced

8.3.5 Advanced: 802.11 b/g Channels

Defines which 802.11b/g channels to use. Only used if the parameter *802.11 b/g channels* is set to "Advanced".

1 Select System > A.

2 Enter channels to scan in a comma-separated list, for example 1,6,11 (the order has no impact, 11,6,1 will give the same result).

8.3.6 Transmit Gratuitous ARP

Some systems require that a gratuitous ARP reply is sent in order to update the ARP table in other devices in the network. Enable *Transmit gratuitous ARP* if reply should be sent when roaming.

1 Select System > A.

2 Select "Enable" in the *Gratuitous ARP* drop-down list.

8.3.7 Transmission Power

This is the transmission power the handset will use when transmitting data to the WLAN system. If "Automatic" is used the transmission power is adapted according to 802.11h, CCX or maximum possible.

1 Select System > A.

2 Select one of the following in the *Transmission power* drop-down list.

- Automatic
- 0 dBm
- 5 dBm
- 11 dBm
- 14 dBm
- Max (20 dBm)

8.3.8 IP DSCP for Voice/Signalling

Differentiated Services Code Point (DSCP) defines which value to use for outgoing voice and signalling traffic. The DSCP value is used for QoS on the LAN. The settings in the handset must agree with the settings in the system, otherwise it will result in bad voice quality.

1 Select System > A.

2 Select one of the following in the *IP DSCP for voice* or *IP DSCP for signalling* drop-down list.

- 0x38 (56) - Class selector 7
- 0x30 (48) - Class selector 6
- 0x2E (46) - Expedited Forwarding
- 0x28 (40) - Class selector 5
- 0x20 (32) - Class selector 4
- 0x1A (26) - Assured forwarding 31
- 0x18 (24) - Class selector 3
- 0x10 (16) - Class selector 2
- 0x08 (8) - Class selector 1
- 0x00 (0) - Default 0

8.3.9 TSPEC Call Admission Control

Defines if Call Admission Control via WMM TSPECs (Traffic Specification) shall be used or not on the WLAN.

1 Select System > A.

2 Select one of the following in the *TSPEC Call Admission Control* drop-down list.

- Disable - Call Admission Control will not be used.
- Auto enable[1] - Call Admission Control will be used if Call Admission Control is mandatory for the WLAN infrastructure.
- Force enable[1] - Call Admission Control will always be used.

8.4 Security Settings

The WLAN system can be configured to use various encryption and/or authentication schemes. The use of extensive encryption/authentication schemes can cause incidents of dropped speech during handover due to the time to process the authentication.

1. The WLAN infrastructure must support the use of TSPEC.

8.4.1 OPEN with or without WEP Encryption

To select OPEN as the security mode. Do the following:

1 Select System > A.

2 Select "OPEN" in the *Security mode* drop-down list.

3 Select "NONE", "WEP64" or "WEP128" in the *Encryption type* drop-down list.

4 If WEP64 or WEP128 encryption is used, select "WEP key X" in the *WEP transmit key* drop-down list.

5 Enter the WEP key X (in hexadecimal format) for the WLAN in the *WEP key X* field.

Note: The *WEP transmit key* decides which key the handset is using for transmitting.

8.4.2 WPA-PSK

To select WPA-PSK as the security mode. Do the following:

1 Select System > A.

2 Select "WPA-PSK" in the *Security mode* drop-down list.

3 Select "TKIP" or "AES-CCMP" in the *Encryption type* drop-down list.

4 Enter the passphrase for WPA-PSK in the *WPA-PSK passphrase* field.

Note: AES-CCMP can be used but is not supported by all systems.

8.4.3 WPA2-PSK

To select WPA2-PSK as the security mode. Do the following:

1 Select System > A.

2 Select "WPA2-PSK" in the *Security mode* drop-down list.

3 Select "AES-CCMP" in the *Encryption type* drop-down list.

4 Enter the passphrase for WPA-PSK in the *WPA-PSK passphrase* field.

8.4.4 802.1X with LEAP

To select LEAP as the authentication method. Do the following:

1 Select System > A.

2 Select "LEAP" in the *Security mode* drop-down list.

3 Select "WEP64", "WEP128" or "TKIP" in the *Encryption type* drop-down list.

4 Enter the user name for EAP authentication in the *EAP authentication user name* field.

5 Enter the password for EAP authentication in the *EAP authentication password* field.

8.4.5 802.1X with PEAP-MSCHAPv2

To select PEAP-MSCHAPv2 as the authentication method. Do the following:

1 Select System > A.

2 Select "PEAP-MSCHAPv2" in the *Security mode* drop-down list.

3 Select "TKIP" or "AES-CCMP" in the *Encryption type* drop-down list.

4 Enter the user name for EAP authentication in the *EAP authentication user name* field.

5 Enter the password for EAP authentication in the *EAP authentication password* field.

8.4.6 802.1X with EAP-MD5

To select EAP-MD5 as the authentication method. EAP does not generate any encryption key material. Do the following:

1 Select System > A.

2 Select "EAP-MD5" in the *Security mode* drop-down list.

3 Select "NONE", "WEP64" or "WEP128" in the *Encryption type* drop-down list.

4 Enter the user name for EAP authentication in the *EAP authentication user name* field.

5 Enter the password for EAP authentication in the *EAP authentication password* field.

6 If WEP64 or WEP128 encryption is used, select "WEP key X" in the *WEP transmit key* drop-down list.

7 Enter the WEP key X (in hexadecimal format) for the WLAN in the *WEP key X* field.

Note: The *WEP transmit key* decides which key the handset is using for transmitting.

8.4.7 Advanced Security Mode

Advanced security mode is only used when it is necessary to have full flexibility of the configuration. It is recommended to use the predefined settings in the *Security mode* drop-down list.

Note: Advanced parameters only have effect if "Advanced" is selected in the *Security mode* drop-down list.

1 Select System > A.

2 Select "Advanced" in the *Security mode* drop-down list, the following advanced items are enabled.

- Advanced: Network association
- Advanced: Network authentication
- Advanced: EAP type
- Advanced: Inner EAP type

8.5 Handset Settings

This section describes specific settings for the handset and these settings can later be changed by the user.

8.5.1 Automatic Key Lock

The automatic key lock is activated when the handset is inactive.

1 Select Device > User.

2 Select "Enable" in the *Automatic key lock* drop-down list.

8.5.2 Rotate New Message

If activated, new messages are displayed 180° rotated.

1 Select Device > User.

2 Select "Enable" in the *rotate new message* drop-down list.

8.5.3 Vibrate During Call

This setting defines how the vibrate function shall work when a message arrives during a call.

1 Select Device > General.

2 Select one of the following in the *Vibrate during call* drop-down list.

- Never vibrate
- Vibrate only on urgency messages
- Always vibrate

8.5.4 Phone Mode

This setting defines if the handset is personal or shared. The default setting is "Personal" but if "Shared" is selected, the handset can be used by several users. Each user can still have their individual settings and access them by personal log in. Shared phone requires a PDM System version.

1 Select Device > General.

2 Select "Personal" or "Shared" in the *Phone mode* drop-down list.

8.5.5 Headset Model

Select the headset model that is used.

1 Select Audio > General.

2 Select the applicable item in the drop-down list:

WARNING! Do not select "Ear protection" unless a Peltor headset is used.

- Mic on boom
- Ear protection
- Mic on cable

8.5.6 Handset Volume

Select the volumes for the different audio signals in the handset.

1 Select Audio > Volume.

2 Select the applicable volume item in the drop-down list:

- Beep volume
- Handsfree volume
- Headset volume
- Handset volume

3 Select "Enable" in the *Persistent volume* drop-down list to automatically store volume changes in the handset for future calls.

8.5.7 Program a Hot Key

A hot key is activated by pressing a preprogrammed button "0" - "9" for more than 1 second. The function is used, for example, to change profile, send message or make a phone call to a specific number.

1 Select HOT KEY and any key number (0-9).

2 Enter function name in the *Hot key name* text field.

3 Enter the applicable index in the *Hot key index* text field. Index parameters are used with the *Hot key functions* "Shortcut", "Presence", "PTT" and "Change profile". See the help text in the PDM for valid indexes.

4 Select one of the following *hot key functions*:

- Disable
- Change profile
- Phone call
- Presence[1]
- PTT
- Send data
- Send data with prefix
- Send message
- Shortcut

5 Enter user data in the *Hot key user data* text field if applicable, see the help text in the PDM.

Continue and repeat the procedure for assigning functions to other hot keys.

1. If the activity ID is changed in the Presence Management system the value for the *Hot key index* in the VoWiFi handset needs to be re-programmed

8.6 Alarm and Messaging

The messaging and alarm functions are provided via the Integrated Message Server IMS/IP-WiFi and described in the document *Installation and Operation Manual, Integrated Message Server IMS/IP-WiFi, TD92322GB*.

8.6.1 IP Address to the IMS/IP-WiFi

The IMS/IP-WiFi handles all communication between the VoWiFi System and the PDM System version. It is required when using the PDM System version.

1 Select Device > Unite.

2 Enter the IP address of the IMS in the *IMS IP address* text field. If left empty, no messaging or alarm function will be available.

8.6.2 Additional Settings for the IMS/IP-WiFi

By entering the following additional settings to the IMS/IP-WiFi, it is possible to send messages from a web browser to a handset, handle messages to groups, send simple messages from handset to handset (and to groups), search for telephone numbers in a central database (on PC), have a central telephone book on the IMS (not PC-based) and to have absence handling in the system.

1 Select Device > Unite.

2 Enter the number that is registered for the user in the IMS in the *IMS phone number* text field.

3 Enter the password in the *IMS phone password* text field.

4 Enter the number of retransmissions in the *Message retransmit limit* text field.

5 Enter the number to the central phonebook directory in the *Central phonebook number* text field to be able to search from the handset.

8.6.3 Message Settings

The time to display a new message is defined by two parameters *Show message time* and *Time to read message*.

If *Time to read message* is set to > 0 this parameter decides how long each message is displayed and the messages received simultaneously are sorted according to priority. If *Time to read message* is set to 0 (zero) the parameter *Show message time* decides how long each message is displayed. Note that if *Time to read message* is set to 0 (zero) the messages are not sorted according to priority.

1 Select UI > Settings.

2 Set the time for how long each new message shall be displayed in the *Show message time* text field.

3 Set the time between showing new messages received simultaneously in the *Time to read message* text field.

4 Select "Small" or "Medium" text size in the *Message text size* drop-down list.

8.6.4 Unread Message Reminder

The user receives a reminder for unread messages in the handset.

1 Select Device > General.

2 Select "Enable" in the *Unread message reminder* drop-down list to activate the reminder.

3 Enter reminder interval in the *Message reminder interval* text field.

8.6.5 Emergency Number

If the *Alarm profile* (Alarm > Emergency call) is set to "Enable" or "Enforce" and the emergency number is called from the handset an alarm is automatically triggered.

1 Select Device > General.

2 Enter the emergency number in the *Emergency number* text field.

8.6.6 Alarm Settings

The following alarm types can be configured; Push-button alarm, Test alarm, Man-down alarm, No-movement alarm and Emergency call.

1 Select Alarm > Common.

2 Enter text to be displayed as pop-up text when the alarm has been sent in the *Status text if alarm OK* text field.

3 Enter text to be displayed as pop-up text if the alarm failed to be sent and is sent again in the *Status text if alarm is resending* text field.

4 Enter text to be displayed as pop-up text if the alarm could not be sent in the *Status text if alarm failed* text field.

5 Enter data to be sent in the alarm block in the *Alarm data* text field.

Alarm Type

This section describes how to configure the alarm button. The procedure is similar for Test alarm, No-movement alarm and Man-down alarm.

1 Select Alarm > Button.

2 Select one of the following in the *alarm profile* drop-down list:

- Disable - The alarm type is disabled.
- Enable - The alarm type is enabled but can be disabled by the user.
- Enforce - The alarm type is enabled and cannot be disabled by the user.

3 Enter number to call in the *Call number after the alarm* text field.

4 Select "Enable" to activate ALS in the *ALS* drop-down list.

5 Enter alarm text in the *alarm type text* field.

6 Select connection method in the *Call after the alarm connection method* drop-down list:

- Monitor - The loudspeaker is muted and the microphone is on.
- Loud - The loudspeaker is turned on.
- Ordinary - The loudspeaker is turned off

Emergency Call

To activate this alarm type the *Emergency number* (Device > General) must also be set.

1 Select Alarm > Emergency call.

2 Select one of the following in the *Alarm profile* drop-down list:

- Disable - The alarm type is disabled.
- Enable - The alarm type is enabled but can be disabled by the user.
- Enforce - The alarm type is enabled and cannot be disabled by the user.

3 Enter alarm text in the *alarm type text* field.

Other settings are not applicable for this alarm type.

Movement Sensor

For the Man-down or No-movement alarm, the following additional settings are available:

1 Select Alarm > Movement sensor.

2 Select "Enable" in the *Extra delay* drop-down list to be able to disable the movement sensor for 10 minutes.

3 Enter time in seconds for the following:

- *Pre-warning time for man down alarm*
- *Pre-warning time for no movement alarm*
- *Time before man down alarm*
- *Time before no movement alarm*

8.7 Telephony

The following parameters are required for the basic telephony settings.

1 Select Device > User.

2 Enter the user number in the *Endpoint number* field.

3 Enter the user ID in the *Endpoint ID* text field.

4 Select Protocols > General.

5 Select "H.323" or "SIP" in the *VoIP Protocol* drop-down list.

8.7.1 Protocol

The protocol is a set of standard rules for data traffic required to send information over a communication channel. Communication protocol is basically following certain rules so that the system works properly.

H.323 Protocol

If the H.323 protocol is used the Gatekeeper IP Address is usually automatically distributed. No configuration necessary.

1 Select Protocols > H.323.

2 The following settings are applicable for the H.323 protocol.

- Gatekeeper IP address
- Secondary Gatekeeper address
- Gatekeeper listening port
- Gatekeeper ID
- Gatekeeper password

SIP Protocol

If the SIP protocol is used the SIP Proxy IP Address must be manually entered.

1 Select Protocols > SIP.

2 The following settings are applicable for the SIP protocol.

- SIP proxy IP address
- Secondary SIP proxy IP address
- SIP proxy listening port
- SIP proxy ID
- SIP proxy password
- Send DTMF using RFC 2833 or SIP INFO – this parameter defines which path the DTMF signalling should take. If set to "RFC 2833", the DTMF signalling will be sent in the RTP stream, i.e. from handset to handset. If set to "SIP INFO", the DTMF signalling will be sent using SIP signalling, i.e. via the PBX.
- Hold type – defines type of hold to send when the handset puts a call on hold. The selection depends on what type of hold the PBX support. For more information about what type of hold the PBX support, see the applicable documentation for the PBX.
- Registration identity – defines if the endpoint shall use its number or ID for the registration with the SIP proxy.
- Authentication identity – defines if the endpoint shall use its number or ID for the authentication with the SIP proxy.
- Call forward locally – when enabled the call forwarding is handled locally by the handset instead of updating the PBX.
  Note: The handset must be switched on and within coverage to handle this.
- MOH locally – Music on hold is played by the handset i.e. if the PBX does not supply MOH the handset plays a tone when the call is on hold.
- Hold on transfer – puts a second call on hold before transfer, which is required by some SIP proxy servers.

8.7.2 Codec

A codec encode a stream or signal for transmission. Codecs are often used in streaming media applications. This setting defines how to packetize and compress the sound in a voice call.

1 Select Protocols > General.

2 Select the applicable codec in the *codec configuration* drop-down list. The following are possible:

- G.711 A-law
- G.711 u-law
- G.729
- G.729A

3 Select packetization time to use for speech in the *Codec packetization time configuration* drop-down list (value between 10 and 60 ms).

8.7.3 Internal Call Number Length

Defines the maximum number of digits to be interpreted as an internal call. "0" means the same number of digits as in the endpoint number.

1 Select Protocols > General.

2 Enter number of digits in the *Internal call number length* text field.

8.7.4 Voice Mail Number

Specifies the number to the Voice Mail box if included in the system.

1 Select Device > General.

2 Enter the number to the voice mail in the *Voice mail number* text field.

8.7.5 Message Centre Number

Specifies the number to the server for Message Waiting Indication (MWI) if included in the system.

1 Select Device > Message centre.

2 Enter the number to the server in the *Message Centre number* text field.

3 Select "Disable" in the *Voice mail call clears MWI* drop-down list to deactivate MWI in the message centre when calling the defined voice mail number.

8.7.6 Max number of Call Completions

Specifies the maximum number of calls to be handled by the handset at the same time before the handset is considered busy.

1 Select Device > General.

2 Enter number of calls in the *Max number of call completions* drop-down list.

8.7.7 Dial Pause Time

By adding a "P" to a phone number, a pause is added and will be activated when dialling. For how long is defined here.

1 Select Device > General.

2 Enter pause time in seconds (1-3) in the *Dial pause time* text field.

8.7.8 Direct off Hook from Charger

The handset will automatically answer a call when removed from the charger.

1 Select Device Device > User.

2 Select "Enable" in the *Direct off hook from charger* drop-down list.

8.7.9 Replace Call Rejected with User Busy

Is used if the system does not support call rejected.

1 Select Device > General.

2 Select "Enable" in the *Replace Call Rejected with User Busy* drop-down list.

8.7.10 In Call Soft Key

This function appears in the display above the right soft key when a call is connected.

1 Select UI > In call soft key.

2 Enter a name in the *In call soft key name* text field.

3 Select one of the following in the *In call soft key action* drop-down list.

- Disabled
- Transfer to new call (blind transfer)
- New call (put active on hold)
- Hold
- Menu
- Transfer (to held call)
- Conference
- Switch
- Retrieve

8.8 Local Settings

This section include settings suitable for a specific region or country.

8.8.1 Set Time & Date

1 Select Device > General.

2 Select the applicable time zone in the *Time zone* drop-down list.

3 Enter the address to the time server in the *NTP server* text field. If not set, the Gatekeeper/SIP proxy address is used.

4 Select UI > Settings.

5 Select the applicable time format in the *Time display format* drop-down list where;

H = Hour
M = Minute

6 Select the applicable date format in the *Date display format* drop-down list where;

Y = Year
M = Month
D = Day

8.8.2 Select Default Language

Defines he default operating language for the handset. This setting can later be changed by the user.

1 Select UI > Settings.

2 Select "Language" in the *Language* drop-down list.

8.8.3 Dialling Tone Pattern

Defines which tone pattern to use when dialling.

1 Select Audio > General.

2 Select the applicable region in the *Dialling tone pattern* drop-down list.

8.9 Display

8.9.1 User Display Text

Defines a text to be shown in the display in idle mode instead of the endpoint ID. If nothing is entered in this text field the endpoint ID will be shown.

1 Select Device > User.

2 Enter the text, in the *User display text* field.

8.9.2 LCD Contrast

Sets the contrast in the display.

1 Select Device > General.

2 Select a contrast value in the *LCD Contrast* drop-down list.

8.9.3 Backlight Timeout

Numbers of seconds before the backlight is turned of.

1 Select Device > General.

2 Enter number of seconds before the backlight is turned of in the *Backlight timeout* text field.

8.9.4 Idle Timeout

Number of seconds before the handset returns to idle mode when in menu mode.

1 Select UI > Settings.

2 Enter number of seconds before the handset returns to idle mode in the *Idle Timeout* field.

8.9.5 Hide Menu Items

It is possible to hide menu items for the users. To hide or show a menu item, do the following:

1 Select UI > Menu items.

2 Select "Hide" or "Show" for the applicable menu item in the drop-down list. The following items can be hidden:

- Alert signals
- Audio volumes
- Alarm settings
- Soft keys
- Hot keys
- General
- Phone lock
- Select system
- Information
- Contacts
- Services
- Call list
- Profiles

8.10 Disable Functions in the Handset

It is possible to disable specific functions for the users. To disable a function, do the following:

1 Select UI > Disable.

2 Select "Enable" or "Disable" for the applicable menu item in the drop-down list. The following are possible:

- Edit hot key
- Delete messages
- Administration of service
- Edit profiles
- Change profile
- Administration of the local phone book

8.11 Shortcut Function Keys

1 Select UI > Settings.

2 Select the applicable function in the drop-down list. The following functions can be set:

- Shortcut Function Key Up (default: Open Message list)
- Shortcut Function Key Down (default: Open Call list)
- Shortcut Function Key Left (default: Open Menu)
- Shortcut Function Key Right (default: Open Menu)

8.12 Configure Profiles

Several profiles are available for the user. Settings as different ring signals and alarm can be set. The profiles is configured via the PDM.

8.12.1 Enter Profile Name

1 In the applicable profile, select Data.

2 Enter a name to identify the profile in the *Profile name* text field.

3 Select "Visible" in the drop-down list to activate this profile.

8.12.2 Edit Profile Settings

1 In the applicable profile, select Settings.

2 Select type of signal in the applicable drop-down list:

- Internal ring signal
- External ring signal
- Callback ring signal

3 Select "Silent" or "Level 1-5" in the *Ring volume* drop-down list.

4 Enable/disable the following functions:

- vibrator
- silent mode
- no movement alarm
- man-down alarm
- manual absent
- key beep

5 Select how to answer in the *Answer mode* drop-down list.

- Ordinary
- Auto
- Loud
- Auto loud

8.12.3 Configure Soft Key

Three soft keys can be configured for each profile.

1 In the applicable profile, select Soft key X.

2 Enter the name of the soft key in the *Soft key name* text field.

3 Enter the applicable index in the *Soft key index* text field. Index parameters are used with the *Soft key functions* "Shortcut", "Presence", "PTT" and "Change profile". See the help text in the PDM for valid indexes.

4 Select the applicable function in the *Soft key function* drop-down list.

- Default
- Disable - no function is used.
- Change profile
- Phone call
- Presence[1]
- PTT
- Send data
- Send data with prefix
- Send message
- Short-cut

5 Enter user data in the *Soft key user data* text field if applicable, see the help text in the PDM.

Repeat the procedure to configure additional soft keys for selected profile.

8.12.4 Diversions

Calls can be diverted to other phone numbers, for example when busy.

1 In the applicable profile, select Diversions.

2 Activate a diversion by selecting "Enable" in the applicable diversion drop-down lists. The following diversions are possible:

- *Activate diversions for all calls*
- *Activate diversions on user busy*
- *Activate no answer diversions*

3 Enter the diversion number in the applicable *diversion number* text field.

8.13 Active Profile

This setting defines the default profile.

1 Select UI > Settings.

2 Select the applicable profile in the *Active profile* drop-down list.

- Normal
- In Charger
- Profile 2
- Profile 3
  :
- Profile 9

1. If the activity ID is changed in the Presence Management system the value for the *Soft key index* in the VoWiFi handset needs to be re-programmed.

8.14 Program a Service

A service is activated from the service menu in the handset.

1 Select Services > and a service number (0-9).

2 Enter the name of the service in the *Service name* text field.

3 Enter the applicable index in the *Service index* text field. See the help text in the PDM for valid indexes.

4 Select one of the following in the *Service function* drop-down list:

- Disable
- Phone call
- Presence[1]
- PTT
- Send data
- Send data with prefix
- Send message

5 Enter user data in the *Service user data* text field if applicable, see the help text in the PDM.

8.15 Presence Management

To be able to configure presence management, the following must be known:

- The IP address to the Presence Management system.
- The user name and password used in the Presence Management system for each handset.

For more information about presence management, see *Function Description, Ascom VoWiFi System, TD 92314GB* or *User Manual i75VoWiFi Handset, TD 92319GB*.

1 Select Presence > Common and choose system in the *Presence Management system* drop-down list.

2 Select Presence > and the Presence Management system selected in previous step.

3 Enter the IP address to the Presence Management system in the *IP address* text field.

4 Enter the number of the port that the Presence Management system shall listen to in the *Listening port* text field.

5 Enter the user name in the *user name* text field.

6 Enter the password in the *password* text field.

The function "Presence" is added to the menu (under Settings) but it can also be assigned to a Soft key, Hot key or Service.

8.16 Location

The location feature requires a 3'rd party location appliance in the system. The handset will scan for access points at defined intervals and, if supported by the system, this will make it possible for the WLAN infrastructure to calculate a position for the handset. The handset will also keep track of the scan result and may transmit collected data to the 3'rd party location appliance. The following must be known:

1. If the activity ID is changed in the Presence Management system the value for the *Service index* in the VoWiFi handset needs to be re-programmed.

- The IP address to the location appliance.
- Which port the location appliance is listening to.

1 Select Location > Common.

2 Enable the *Location scanning* parameter.

3 Set the time between the scanning periods in the *Scanning interval*[1] text field.

4 Select how many scans that should be performed during each scanning period in the *Scans per scanning period*[1] drop-down list.

5 Select applicable location appliance.

6 Enter the IP address to the location appliance in the *IP address* text field.

7 Enter the number of the port the location appliance is listening to, in the *Listening port* text field.

8.17 Push-To-Talk (PTT) Group Call

To be able to configure a PTT session, the following must be known:

- The group number to the PTT group (defined in the IMS/ESS).
- The phone number to the conference bridge.

For more information about the PTT function, see *Function Description, Ascom VoWiFi System, TD 92314GB* or *User Manual i75VoWiFi Handset, TD 92319GB*.

Note: If Music on Hold (MOH) is used in the system it can effect an ongoing PTT group call. If someone in the group conference answers another incoming call, MOH will be played for the whole group.

1 Select Push-To-Talk > PTT X.

2 Enter a name to identify the PTT session in the *Session name* text field.

3 Enter the number to the PTT conference group in the *Group number* text field.

4 Enter a text to be shown in the display during the PTT session in the *Display text* field.

5 Select the indication of the PTT session in the *PTT session signal* drop-down list.

6 Enter the phone number to the conference bridge in the *Conference number* text field.

7 Select the answer mode for the PTT session in the *Answer mode* drop-down list.

8 Select the speaker mode for the PTT session in the *Speaker mode* drop-down list.

The function must be assigned to a Soft key, Hot key or Service.

1.Note that close scanning periods, and frequently scans per period, will shorten the battery time.

9 Use i75 VoWiFi Handset to Verify the VoWiFi System Deployment

We recommend doing site surveys with the built-in tools in the VoWiFi handset. This provides a true measurement of the RF environment based upon the radio of the handset. Other wireless analysers may be used to provide additional assistance during a site survey.

It is recommended to use i75 VoWiFi handset v 1.2 for site surveys. Release v 1.1 has a limited site survey that only shows the strongest AP for each ESSID.

9.1 Scan the Channels

To be able to use the site survey functions in the VoWiFi Handset it must be configured correctly.

Default configuration for the handset is to use channels 1, 6 and 11. If the handset is intended for site survey use, scanning all channels will be limited to 1, 6 and 11. The result is stored in the handset in a table with max. 16 entries. The table is upgraded regularly, starting with scanning channel 1, then 6 and last 11. In between the handset is in sleeping mode. The handset consults this table when making roaming decisions.

To enable scanning of all channels the parameter "802.11b/g channels" should be set to "All". It is strongly recommended to set back the handset to "1,6,11" when in normal use.

The *World mode regulatory domain* will also affect which channels that may be used. To scan channels 1-11 it is recommended that the handset is configured so the "World mode regulatory domain" parameter is set to "USA". If also scanning of channels 12 and 13 is of interest use value "ETSI".

There are three ways of scanning channels:

- Scan all channels
- Scan a specific channel
- Scan for unknown systems

9.1.1 Scan all Channels

This gives a list of the channels in the ESSID found during the scan.

1 Press "*#77#" on the handset to access the site survey menu.

2 Select "Scan all channels".

3 Select the ESSID to display its associated APs.

4 Select an AP to display information such as ESSID, MAC address or QoS.

9.1.2 Scan a Specific Channel

This gives a list of all the APs found on that channel in the specified ESSID.

1 Press "*#77#" on the handset to access the site survey menu.

2 Enter the channel number to scan.

3 Select an AP to display information such as ESSID, MAC address or QoS.

9.1.3 Scan for Unknown System

This gives a list of all existing ESSIDs found during the scan.

1 Create an ESSID which does **not** exists.

2 Enter an descriptive system name.

3 Make sure the handset is personal.

4 Select the previously created system in the handset. "No system" is displayed.

5 Press "*#77#" on the handset to access the site survey menu.

6 Select "Scan all channels" to list all ESSIDs available.

7 Select the applicable ESSID to display its associated APs.

8 Select an AP to display information such as ESSID, MAC address or QoS.

9.2 Range Beep

The range beep function enables a beep to be played whenever the handset experiences a filtered field strength of below the configured value (default -70 dBm) from the currently associated access point. Since the value is filtered, sudden drops in field strength caused by the environment, for example walking through a door into a room, will be delayed, thus it is important to walk slowly through the site to cover all weak spots.

9.2.1 Configurable Roaming Threshold

Since the roaming threshold of the handset is set at the same value as the range beep (-70 dBm) each roam will cause a small period of beeping. In the site survey menu there is the possibility to change the roaming/low RSSI threshold. This is useful if a specific area is designed to have another coverage level than -70 dBm.

In normal operation the handset uses -70 dBm, it is very important to change this value back to -70 dBm (or simply reboot the handset) before validating the rest of the system.

1 Press "*#77#" on the handset to access the site survey menu.

2 Select "Range level"

3 Enter the new threshold and press "Set".

9.2.2 Range Beep on a Configurable Roaming Threshold

A beep is played when the signal goes below the selected threshold.

1 Press "*#77#" on the handset to access the site survey menu.

2 Enable/Disable the *Range beep* checkbox.

10 VoWiFi Handset Internal Web Administration Page

The internal web administration page for the handset makes it possible to:

- Download licences[1] for the alarm and location features, refer to 6 *Add Alarm Features* on page 11 and 7 *Add Location Features* on page 12.
- Upgrade software, refer to 12 *Upgrade the Software* on page 38.
- Troubleshoot the VoWiFi System.
- View statistics, see below.

10.1 Access the Handset´s Internal Web Administration page

1 Enter the handset´s IP address in the address bar in the web browser to access the internal web administration page for the handset. The IP address can be found in the handset´s menu (Settings >System >Information).

The web administration page opens is the System Setup information view. The following are shown:

- Software version
- MAC address
- Coder
- SNTP server
- Local time
- Uptime

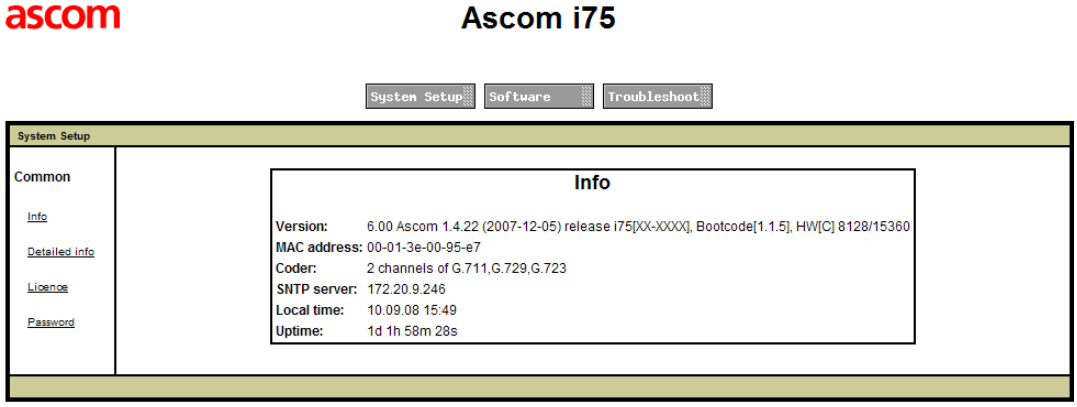

Figure 2. The information view

2 Enter administration user name and administration password to access further pages.

Default user name and password for an administrator:

- User name: admin
- Password: changeme

10.1.1 Show Detailed Information

1 Click the *Detailed info* link. The following information is shown:

- IP address
- Subnet mask
- Default gateway
- SIP proxy/H.323 gatekeeper IP address

1.Note that licences are associated with the handset, i.e. a new/replaced handset must be upgraded

10.2 Change Administration Password

The administration password can be changed either via the i75 internal Web Administration page or via the PDM.

Change password via the VoWiFi Handset´s Internal Web Administration page

1 Access the Web Administration page, refer to 10.1 *Access the Handset´s Internal Web Administration page* on page 33.

1 Enter administration user name and administration password.

- Default user name: admin
- Default password: changeme

2 Click the "Password" link.

3 Enter the new user name in the *User* text field.

4 Enter the new password in the *Password* text field.

5 Con firm the new password and click the "Change" button.

Change password via the PDM

1 Open the PDM.

1 Select Device > General.

2 Enter user name in the *Administration user name* text field.

3 Enter password in the *Administration password* text field.

11 Troubleshooting

11.1 Display Information and Symptoms in the VoWiFi Handset

11.1.1 "No system"

When the i75 shows "No system" it cannot find the wireless infrastructure with settings matching those configured in the handset.

1 Check the ESSID. The ESSID configured in the handset must be identical to the ESSID configured in the system infrastructure.

2 Check the security settings. The security settings i.e. authentication and encryption must match the settings in the system infrastructure.

3 Check for 802.11d multi regulatory domain settings. The VoWiFi handset version 1.1.0 – 1.1.15 must be able to detect in which country it is located to use the correct channel and transmit power settings. Later versions have a parameter specifying if 802.11d should be used or not. This is provided by the infrastructure according to the 802.11d standard.

4 Check which channels are used. The VoWiFi handset uses by default channel 1, 6 and 11. If the infrastructure is configured to use any other channel, change it to use only 1, 6 and 11 as this is the recommended setting.

5 Check that the correct system (A, B, C or D) setting is selected.

11.1.2 "No access"

When the handset shows "No access" it has found and associated to the WLAN (a wireless network with the configured ESSID and correct security settings). But it can connect to neither the gatekeeper nor the messaging gateway (IMS/IP-WiFi).

1 Check if the handset has an IP address by entering the "System information" screen. If not check the WEP key if used or WPA/WPA2 passphrase.

2 If using WEP double-check the key if the handset has no IP address. If you have a wireless sniffer, configure it to the correct key and try to decode packets both from and to the handset.

3 Check the Gateway address. Try to ping the gateway from another wireless client.

4 Check the IMS address. Try to ping the IMS from another wireless client.

11.1.3 "Voice only"

When the handset shows "Voice only" it is configured to use both a gatekeeper and an IMS/IP-WiFi, but has lost contact with the IMS/IP-WiFi.

1 Check the IMS/IP-WiFi address. Try to ping the IMS from another wireless client.

2 Remove i75 handset from PDM stand alone programming device. When connected to the PDM Windows version via USB, the handset cannot connect to the IMS and may then show "Voice only".

3 If messaging is not used in the system, verify that the IMS address is configured to 0.0.0.0.

11.1.4 “Messaging only”

When the handset shows “Messaging only” it is configured to use both a gatekeeper and an IMS/IP-WiFi, but has lost contact with the gatekeeper.

1 Check the Gateway address. Try to ping the gateway from another wireless client.

2 Try to send a message. The idle connection check interval to the IMS/IP-WiFi is much longer than to the gateway. Sometimes when all network connection is lost the handset will show “Messaging only” for quite some time, because it discovers it has lost connection to the gateway much faster than it discovers loss of connection to the IMS/IP-WiFi. In this case the i75 will eventually change to “No access”.

3 If the phone is supposed to use Gatekeeper discovery, verify that the configured Gatekeeper IP address is 0.0.0.0.

4 Check the Endpoint number and the Endpoint ID. If both are configured the MUST match each other. Try clearing one of them.

11.1.5 Voice Quality is Bad

1 Check if QoS is working in both directions. Voice traffic should be prioritized on both the LAN and the WLAN.

2 Connect to other phones (wired, analogue or external) to determine if it is the other end that may cause bad quality.

3 Do a site survey and check for areas with under/over coverage and other interfering 802.11 systems.

4 Do a network performance test to ensure the wired LAN/backbone has adequate capacity.

5 Use a spectrum analyser and look for non 802.11 interference.

11.1.6 Battery Life is Bad

1 Check “Beacon interval” and “DTIM” settings in the AP.

2 Verify the coverage, since low signal strength will make the handset to constantly search for other APs and thereby consuming more power.

3 Use a sniffer and check the amount of broadcast traffic that is transmitted on the WLAN.

4 Check if correct models of the chargers are used.

5 Verify with another battery.

6 If the system is supposed to use U-APSD for voice calls check the voice power save mode parameter in the PDM.

11.1.7 Connected Call but No Sound or One Way Sound

1 Note the IP address of the handset. Turn the handset off and ping the IP address. If something is found, the problem is an IP address conflict.

2 Check if the handsets are muted.

3 Use a headset to eliminate bad speakers/microphone.

11.2 Quick Access to the VoWiFi Handset´s Basic Settings

To identify some basic settings, enter the following code in the handset.

Setting	Code
IP address	*#46#
MAC address	*#46#
Software version	*#46#
Current ESSID	*#46# or *#76#
Current BSSID	*#76#
Current RSSI	*#76#
Current channel	*#76#
Site survey functions	*#77#
Currently used transmit speed	A Hot key or Soft key can be programmed as a short-cut for Network statistics.
Total transmit failures	A Hot key or Soft key can be programmed as a short-cut for Network statistics.

Note: Other settings and information can be found on the i75 internal web administration page, refer to chapter 10 *VoWiFi Handset Internal Web Administration Page* on page 33.

11.3 Troubleshooting from the i75 Internal Web Administration Page

It is possible to view statistics for Voice and WLAN connectivity and to create debug and error logs from the i75 internal web administration page. The logs and the statistics can then be interpreted by your supplier.

1 Access the VoWiFi internal web page, refer to 10.1 *Access the Handset´s Internal Web Administration page* on page 33.

2 Click the *Troubleshoot* button.

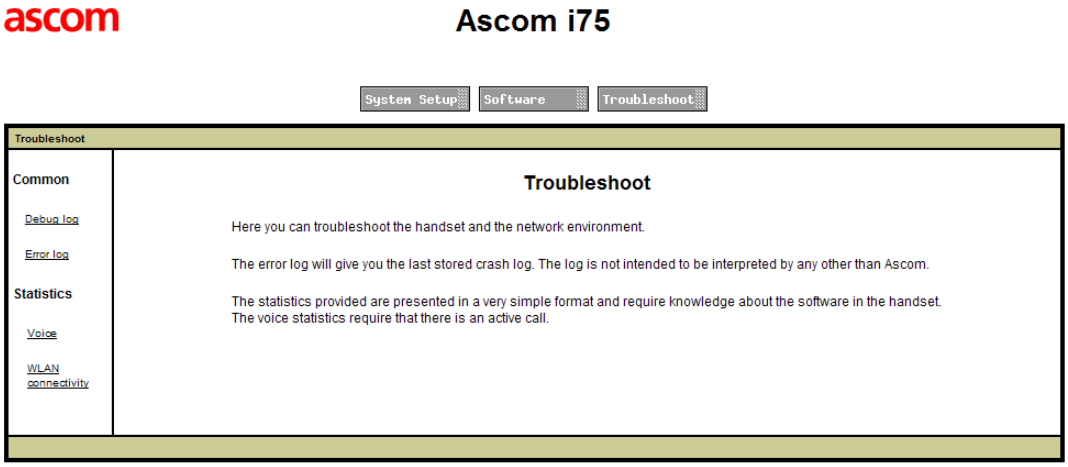

Figure 3. Troubleshoot page

12 Upgrade the Software

Note: Pay attention to the software Release Notes before changing the software. Note especially that the i75 Messenger version is not compatible with software versions previous to 1.5.8.

The software in the Ascom i75 VoWiFi handset can be upgraded either via the i75 internal Web Administration page or via the PDM. For software upgrade via the PDM refer to the applicable *PDM Installation and Operation Manual*.

Note: The fastest and most reliable way is to use the PDM for the software upgrade.

12.1 Upgrade SW via the VoWiFi Handset´s Internal Web Administration page

1 Access the Web Administration page, refer to 10.1 *Access the Handset´s Internal Web Administration page* on page 33.

2 Click the "Software" button.

3 Enter the path and file name of the software file to be loaded, or click "Browse".

4 Click the "Upgrade" button.

Note: The handset will always use the latest downloaded software at startup but, as described below, it can be forced to use another version.

12.2 Recapture the earlier Software

The handset stores two software versions which makes it possible to force the handset to jump back to the earlier software, if necessary.

Note: The handset must be switched off to be able to load the earlier software.

1 Press and hold the keys “7” and “8” and press On/Off key at the same time.

The handset loads the earlier software and will keep it as long it is not restarted.

13 Related Documents

Data Sheet, Ascom i75 VoWiFi Handset	TD 92318GB
User Manual i75VoWiFi Handset	TD 92319GB
Function Description, Ascom VoWiFi System	TD 92314GB
Considerations for Ascom VoWiFi System Planning	TD 92408GB
Installation and Operation Manual Phonebook Service	TD 92360GB
Installation and Operation Manual, Portable Device Manager (PDM), Windows version	TD 92325GB
Installation and Operation Manual, Portable Device Manager (PDM), System version	TD 92378GB

14 Document History

For details in the latest version, see change bars in the document.

Version	Date	Description
A	2007-10-22	First Released version
B	2008-11-20	New parameters: • 8.3.5 *Advanced: 802.11 b/g Channels* on page 14 • 8.7.3 *Internal Call Number Length* on page 23 • 8.16 *Location* on page 29 New settings in *SIP Protocol* on page 22 New chapters: • 7 *Add Location Features* on page 12 • 10 *VoWiFi Handset Internal Web Administration Page* on page 33. • 11.3 *Troubleshooting from the i75 Internal Web Administration Page* on page 37. • 12.1 *Upgrade SW via the VoWiFi Handset's Internal Web Administration page* on page 38.